แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ของสำนักงานนโยบายและแผนการขนส่งและจราจร

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
ธันวาคม ๒๕๖๓

คำนำ

ข้อมูลสารสนเทศถือเป็นทรัพยากรที่มีความสำคัญยิ่งต่อการปฏิบัติงานราชการและการบริหารราชการของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) ดังนั้น จึงจำเป็นต้องได้รับการดูแลและบำรุงรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

สนข. ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศที่อาจประสบกับความเสียหายจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่าง ๆ ในการนี้ ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.) จึงได้ทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ประจำปีงบประมาณ พ.ศ. ๒๕๖๓ เพื่อจัดทำ IT Contingency Plan ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ให้มีความเหมาะสม ทันสมัย สอดคล้องกับสถานการณ์ ศทท. หวังเป็นอย่างยิ่งว่า IT Contingency Plan ฉบับนี้ จะเป็นกรอบแนวทางเพื่อเตรียมความพร้อมในการป้องกัน แก้ไขปัญหาและลดผลกระทบจากสถานการณ์ความไม่แน่นอนอันอาจส่งผลเสียหายต่อฐานข้อมูลและเทคโนโลยีสารสนเทศในภาพรวมของ สนข.

การฝึกปฏิบัติตาม IT Contingency Plan ครั้งนี้ เป็นการฝึกปฏิบัติการแบบทั่วทั้งองค์กร ในกรณีกระแสไฟฟ้าขัดข้องและกรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี โดยมี ศทท. เป็นหน่วยงานหลัก และบุคลากรของ สนข. มีส่วนร่วมในการฝึกปฏิบัติการฯ ซึ่ง ศทท. หวังเป็นอย่างยิ่งว่า IT Contingency Plan และการฝึกปฏิบัติการดังกล่าวจะเป็นประโยชน์ต่อเจ้าหน้าที่ผู้รับผิดชอบในการปฏิบัติการด้าน IT โดยตรง รวมทั้ง เป็นประโยชน์ต่อเจ้าหน้าที่ สนข. ที่ใช้ระบบ IT ในการปฏิบัติงาน

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
ธันวาคม ๒๕๖๓

สารบัญ

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

ปัจจุบันภัยที่เกิดกับระบบเทคโนโลยีสารสนเทศ (Information Technology : IT) มีอัตราการเกิดเพิ่มขึ้นตามความก้าวหน้าของ IT ภัยอันตรายที่อาจเกิดขึ้นกับระบบ IT อาจเกิดขึ้นได้โดยคน เช่น เจ้าหน้าที่บุคลากรของหน่วยงานที่เกี่ยวข้องกับการใช้งาน IT สถานการณ์หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนาอันเป็นเหตุให้ข้อมูลข่าวสารในระบบ IT ถูกเปิดเผย หรือเปลี่ยนแปลงทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่น ๆ ตามความต้องการของภัยเป็นต้น ดังนั้น เพื่อเป็นการลดภัยดังกล่าวที่จะเกิดขึ้นในระบบ IT ของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้าน IT ของ สนข. เพื่อรองรับสถานการณ์ดังกล่าวที่อาจจะเกิดขึ้นกับระบบ IT

๑.๒ วัตถุประสงค์

จัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ เพื่อใช้เป็นกรอบแนวทางสำหรับการเตรียมความพร้อมในการป้องกัน แก้ไขปัญหา และลดผลกระทบจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น

๑.๓ เป้าหมาย

เพื่อลดความเสียหายที่จะเกิดกับระบบ IT ของ สนข. และเพื่อให้ระบบ IT ของ สนข. สามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้ง เตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบ IT ของ สนข.

๑.๔ ประโยชน์ที่คาดว่าจะได้รับ

ระบบคอมพิวเตอร์พร้อมอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์ของ สนข. สามารถกู้คืนให้กลับมาใช้งานได้อย่างต่อเนื่องภายในระยะเวลาที่เหมาะสมตามที่กำหนดไว้ภายหลังจากเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติด้าน IT

๑.๕ ผู้รับผิดชอบ

<u>ที่ปรึกษา</u>

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร สนข.

<u>ผู้ปฏิบัติงาน</u> กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย

๑. นายสมชาย ภูนาสี	หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย	โทร. ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๕๑๔
๒. นางสาวนิปริน คำแสง	นักวิชาการคอมพิวเตอร์ชำนาญการ	โทร. ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๘๑
๓. นายนฤทธิ์ มัยรัตน์	นักวิชาการคอมพิวเตอร์ชำนาญการ	โทร. ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๕๑๕
๔. นายพิสิฏฐ์ ป้อมทอง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	โทร. ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๑๒
๕. นายชัยวัฒน์ ธรรมาสถิตนุกุล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	โทร. ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๑๔
๖. นายทนงชัย ยศชัยพงศ์	นายช่างเขียนแบบชำนาญงาน	โทร. ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๕๑๓
๗. นายพิสุทธิ นิลม่วง	พนักงานบริการเอกสารทั่วไป ระดับ ปวช	โทร. ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๕๑๓

บทที่ ๒

การทบทวนและประเมินสถานการณ์ความไม่แน่นอนและภัยพิบัติด้าน IT ที่อาจเกิดขึ้น และแนวทางปฏิบัติ

๒.๑ การทบทวนผลการฝึกปฏิบัติตาม IT Contingency Plan ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๒

๒.๑.๑ ศทท. ได้ฝึกปฏิบัติการในสถานการณ์จำลองตาม IT Contingency Plan ดังกล่าว โดยได้ฝึกปฏิบัติกรณีกระแสไฟฟ้าขัดข้อง เมื่อวันที่ ๑๔ กรกฎาคม ๒๕๖๓ ช่วงเวลา ๑๑.๐๐ - ๑๒.๐๐ น. และได้ฝึกปฏิบัติกรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตีเมื่อวันที่ ๑๔ สิงหาคม ๒๕๖๓ ระหว่างเวลา ๑๑.๐๐ - ๑๒.๐๐ น.

๒.๑.๑.๑ สำหรับการฝึกปฏิบัติการกรณีกระแสไฟฟ้าขัดข้อง ได้ดำเนินการโดยปิดสวิตช์เพื่อตัดกระแสไฟฟ้าหลักที่จ่ายเข้าห้องศูนย์ข้อมูล แล้วจึงปิดเครื่อง Server อุปกรณ์เครือข่าย และ UPS ตามลำดับ และได้เปิดสวิตช์ไฟฟ้าหลักเพื่อปล่อยกระแสไฟฟ้าเข้าสู่ห้องศูนย์ข้อมูล แล้วจึงเปิด UPS อุปกรณ์ระบบเครือข่าย และเครื่อง Server ให้กลับมาใช้ในการปฏิบัติงานได้ตามปกติ พบว่า ภาพรวมในการฝึกปฏิบัติการฯ สามารถดำเนินการฝึกได้ครบทุกกระบวนการภายในระยะเวลาไม่เกิน ๔๐ นาที ซึ่งเป็นระยะเวลาที่เครื่อง UPS ยังสามารถจ่ายกระแสไฟฟ้าสำรองได้อย่างต่อเนื่อง จึงทำให้อุปกรณ์และระบบเครือข่ายคอมพิวเตอร์ของ สนข. สามารถลดความเสี่ยงและความเสียหายจากกระแสไฟฟ้าขัดข้องได้ รวมทั้ง ได้รับการป้องกันและช่วยลดปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์ได้ ช่วยให้สามารถกู้คืนระบบคอมพิวเตอร์พร้อมอุปกรณ์และระบบเครือข่ายคอมพิวเตอร์ได้อย่างทันท่วงที และเมื่อเปรียบเทียบการฝึกปฏิบัติการฯ เมื่อปีงบประมาณ พ.ศ. ๒๕๕๘ พ.ศ. ๒๕๕๙ พ.ศ. ๒๕๖๐ (ครั้งที่ ๑ และครั้งที่ ๒) และ พ.ศ. ๒๕๖๑ (ครั้งที่ ๑ และครั้งที่ ๒) พ.ศ. ๒๕๖๒ (ครั้งที่ ๑ และครั้งที่ ๒) และ พ.ศ. ๒๕๖๓ (ครั้งที่ ๑ และครั้งที่ ๒) แสดงผลการฝึกปฏิบัติได้ดังนี้

ปีงบประมาณ	กิจกรรม	ระยะเวลาที่ใช้ในการปิดระบบ	ระยะเวลาที่ใช้ในการเปิดระบบ
พ.ศ. ๒๕๕๘	ครั้งที่ ๑ กรณีกระแสไฟฟ้าขัดข้อง	ประมาณ ๔๐ นาที	ประมาณ ๕๕ นาที
พ.ศ. ๒๕๕๙	ครั้งที่ ๑ กรณีกระแสไฟฟ้าขัดข้อง	ประมาณ ๔๐ นาที	ประมาณ ๕๕ นาที
พ.ศ. ๒๕๖๐	ครั้งที่ ๑ กรณีกระแสไฟฟ้าขัดข้อง	ประมาณ ๒๐ นาที	ประมาณ ๑๕ นาที
	ครั้งที่ ๒ กรณีกระแสไฟฟ้าขัดข้อง	ประมาณ ๒๐ นาที	ประมาณ ๑๕ นาที
พ.ศ. ๒๕๖๑	ครั้งที่ ๑ กรณีกระแสไฟฟ้าขัดข้อง	ประมาณ ๒๐ นาที	ประมาณ ๑๕ นาที
	ครั้งที่ ๒ กรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี	ระยะเวลาที่ใช้ในการฝึกปฏิบัติการฯ ประมาณ ๖๐ นาที	
พ.ศ. ๒๕๖๒	ครั้งที่ ๑ กรณีกระแสไฟฟ้าขัดข้อง	ประมาณ ๒๐ นาที	ประมาณ ๑๕ นาที
	ครั้งที่ ๒ กรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี	ระยะเวลาที่ใช้ในการฝึกปฏิบัติการฯ ประมาณ ๖๐ นาที	
พ.ศ. ๒๕๖๓	ครั้งที่ ๑ กรณีกระแสไฟฟ้าขัดข้อง	ประมาณ ๒๐ นาที	ประมาณ ๑๕ นาที
	ครั้งที่ ๒ กรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี	ระยะเวลาที่ใช้ในการฝึกปฏิบัติการฯ ประมาณ ๖๐ นาที	

๒.๑.๑.๒ สำหรับการฝึกปฏิบัติกรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี ได้ดำเนินการ ดังนี้

(๑) เจ้าหน้าที่ ศทท. ท่านหนึ่ง ได้โทรฯ หาเจ้าหน้าที่ ศทท. (กพค.) เพื่อให้เจ้าหน้าที่ ศทท. (กพค.) ตรวจสอบเครื่องคอมพิวเตอร์ดังกล่าว

(๒) เจ้าหน้าที่ ศทท. (กพค.) ได้ตรวจสอบเครื่องคอมพิวเตอร์ดังกล่าวแล้ว พบว่าไวรัสดังกล่าวเป็นไวรัสชนิด Ransomware ซึ่งแพร่กระจายผ่านทางระบบเครือข่ายคอมพิวเตอร์ และเป็นไวรัสชนิดที่โปรแกรม Antivirus ในปัจจุบันไม่สามารถตรวจพบได้ จึงต้องทำการดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์ดังกล่าวโดยเร็ว

(๓) ประกาศแจ้งบุคลากรของ สนข. ทุกท่านว่า “ขณะนี้เป็นการจำลองสถานการณ์การติดไวรัสของครื่องคอมพิวเตอร์ของเจ้าหน้าที่ ศทท. ท่านหนึ่ง จึงขอให้เจ้าหน้าที่ สนข. ทุกท่าน โปรดตรวจสอบระบบคอมพิวเตอร์ของตนเองว่า มีสิ่งผิดปกติหรือไม่ เช่น แสดงข้อความ Digital file ที่ผิดปกติ หรือไม่รู้จักแหล่งที่มา หรือเครื่องคอมพิวเตอร์ของท่านทำงานผิดปกติไปจากเดิม” ซึ่งไม่พบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม

(๔) เจ้าหน้าที่ ศทท. (กพค.) ดำเนินการ Format เครื่องที่ติดไวรัส แล้วดำเนินการดังนี้

(๔.๑) ติดตั้งระบบปฏิบัติการ และระบบเครือข่าย รวมทั้งโปรแกรมประยุกต์ที่จำเป็นต่อการใช้งาน พร้อมทั้งเสียบสาย LAN

(๔.๒) นำข้อมูลที่ Backup ไว้มาทำการ Recovery เพื่อนำข้อมูลเดิมกลับมาใช้

(๔.๓) ตรวจสอบและเปิดเครื่องคอมพิวเตอร์ให้ทำงานตามปกติ

(๕) ประกาศแจ้งสิ้นสุดการจำลองสถานการณ์ เพื่อให้บุคลากรของ สนข. ทำงานได้ตามปกติ

๒.๑.๒ การทบทวนใช้หลักการการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและข้อมูลการประเมินความเสี่ยงจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) จำแนกความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. มีดังนี้

ลำดับที่	ความเสี่ยง	ประเภทความเสี่ยง	ระดับโอกาสที่จะเกิดขึ้น (a)	ระดับผลกระทบ (b)	คะแนนรวม (a x b)	
๑	ถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี	๕	๕	๕	๒๕	สูงมาก
๒	ซอฟต์แวร์ระบบฐานข้อมูล/โปรแกรมหรือแอพพลิเคชั่นเสียหาย	๒	๔	๕	๒๐	สูง
๓	ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า	๓	๔	๔	๑๖	
๔	การเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต	๕	๓	๕	๑๕	
๕	อุปกรณ์คอมพิวเตอร์ชำรุดเสียหาย	๑	๒	๕	๑๐	ปานกลาง
๖	การใช้งานระบบซอฟต์แวร์เถื่อนหรือซอฟต์แวร์ละเมิดลิขสิทธิ์	๖	๓	๓	๙	
๗	ระบบเครือข่ายหลักเสียหาย/ขัดข้องไม่สามารถใช้งานได้	๔	๒	๓	๖	
๘	การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data room)	๓	๑	๕	๕	
๙	ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า แผ่นดินไหว และน้ำท่วม)	๓	๑	๕	๕	
๑๐	ระบบคอมพิวเตอร์ถูกเจาะ (Hack)	๕	๑	๕	๕	
๑๑	การใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ผิดวัตถุประสงค์	๖	๕	๑	๕	

ลำดับที่	ความเสี่ยง	ประเภทความเสี่ยง	ระดับโอกาสที่จะเกิดขึ้น (a)	ระดับผลกระทบ (b)	คะแนนรวม (a x b)	
๑๒	อุปกรณ์คอมพิวเตอร์ถูกขโมย	๑	๑	๕	๕	ปานกลาง
๑๓	การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์	๕	๑	๔	๔	
๑๔	เครื่องปรับอากาศห้องศูนย์ข้อมูลไม่ทำงาน	๓	๑	๔	๔	
๑๕	การก่อความไม่สงบ/จลาจล	๕	๑	๓	๓	

หมายเหตุ

• ประเภทความเสี่ยง :

๑ หมายถึง ความเสี่ยงด้าน Hardware
๒ หมายถึง ความเสี่ยงด้าน Software
๓ หมายถึง ความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ
๔ หมายถึง ความเสี่ยงด้านระบบเครือข่ายและ Internet
๕ หมายถึง ความเสี่ยงด้านความมั่นคงปลอดภัย
๖ หมายถึง ความเสี่ยงด้านตัวบุคคลและการใช้งาน

• ระดับโอกาสที่จะเกิดขึ้นและระดับผลกระทบ :

๑ หมายถึง น้อยมาก
๒ หมายถึง น้อย
๓ หมายถึง ปานกลาง
๔ หมายถึง สูง
๕ หมายถึง สูงมาก

๒.๑.๓ จากผลการทบทวน IT Contingency Plan ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๒ ศทท. เห็นว่าความเสี่ยงจากกรณีกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้าเป็นประเภทความเสี่ยงที่อาจเกิดขึ้นได้ มีผลกระทบสูงและสร้างความเสียหายให้กับระบบเทคโนโลยีสารสนเทศของ สนข. รวมทั้ง การฝึกปฏิบัติไม่ยุ่งยากเกินไป สามารถปฏิบัติจริงได้ในระยะเวลาที่กำหนด จึงเห็นควรบรรจุการฝึกปฏิบัติในด้านกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า และกรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตีไว้ใน IT Contingency Plan ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๓

๒.๒ การประเมินสถานการณ์ความไม่แน่นอนและภัยพิบัติด้าน IT ที่อาจเกิดขึ้นและแนวทางปฏิบัติ

จากการติดตามตรวจสอบสถานการณ์ความไม่แน่นอนและภัยพิบัติต่าง ๆ ในระบบ IT ของ สนข. พบว่าสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเป็นอันตรายต่อระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบ IT ของ สนข. สามารถแยกเป็นภัยพิบัติที่เกิดจากความเสี่ยงต่าง ๆ ได้ ๖ ประเภท ดังนี้

ลำดับที่	ภัยพิบัติ	แนวทางปฏิบัติ/มาตรการควบคุม
๑	**ภัยพิบัติที่เกิดจากความเสี่ยงด้าน Hardware** เช่น อุปกรณ์คอมพิวเตอร์ชำรุดเสียหาย และอุปกรณ์คอมพิวเตอร์ถูกขโมย	ศทท. มีมาตรการควบคุม ดังนี้ (๑) ภายในห้องศูนย์ข้อมูล (Data room) การเข้าออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่ายหากจำเป็นให้มีเจ้าหน้าที่ของกลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจรเป็นผู้รับผิดชอบนำพาบุคคลเข้าไปผ่านประตูเข้าออกซึ่งมีการติดตั้งเครื่องสแกนลายนิ้วมือ รวมทั้ง ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพื่อบันทึกการเข้า - ออก และการปฏิบัติงานในห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายด้วย
		(๒) ภายนอกห้องศูนย์ข้อมูล (Data room) ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย CCTV และ Access control ทุก ๖ เดือน (๓) สำรองข้อมูลแบบ Full Backup และแบบ Incremental
๒	ภัยพิบัติที่เกิดจากความเสี่ยงด้าน Software เช่น ซอฟต์แวร์ระบบฐานข้อมูล/โปรแกรมหรือแอปพลิเคชันเสียหาย	ศทท. ได้ทำการติดตั้งอุปกรณ์ป้องกันการบุกรุกเข้าสู่ระบบเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Firewall) ซึ่งเป็นอุปกรณ์ที่ทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก เพื่อป้องกันบุคคลมิให้เข้าถึงหรือสร้างความเสียหายแก่ระบบฐานข้อมูล รวมทั้ง หมั่นตรวจสอบ Policy และ Log ของ Firewall และ IPS/IDS อย่างสม่ำเสมอ และจัดทำระบบป้องกันการเข้าถึงห้องศูนย์ข้อมูล โดยอนุญาตเฉพาะเจ้าหน้าที่ผู้เกี่ยวข้องกับการบริหารจัดการเครื่อง Server และเจ้าหน้าที่ที่มีสิทธิ์เข้าใช้งานภายในห้องศูนย์ข้อมูล รวมทั้ง ติดตั้งระบบกล้อง CCTV เพื่อบันทึกภาพการเข้าออกภายในห้องไว้ด้วย และ ศทท. ได้มีการหมั่นตรวจสอบระบบคอมพิวเตอร์แม่ข่ายฐานข้อมูลหลักและมีการสำรองข้อมูลฐานข้อมูล นอกจากนี้ยังมีการติดตั้ง Software ป้องกันมัลแวร์ที่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ลูกข่าย (Client) ซึ่งทำหน้าที่ดักจับมัลแวร์ที่เข้ามาในระบบเครือข่ายและสามารถตรวจสอบได้ว่ามีมัลแวร์ชนิดใดที่เข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ของ สนข. และผู้ใช้งานระบบ IT ต้องดำเนินการดังนี้ (๑) Update ข้อมูลป้องกันมัลแวร์อยู่เสมอ (๒) ใช้โปรแกรมเพื่อทำการตรวจหาป้องกันมัลแวร์โดยการ Scan มัลแวร์อย่างน้อยสัปดาห์ละ ๑ ครั้ง (๓) Scan มัลแวร์ทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูลต่าง ๆ เช่น แผ่นดิสก์ แผ่นซีดี และ Handy drive/Thumb drive เป็นต้น (๔) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลก ๆ ที่ไม่รู้จักหรือน่าสงสัย เช่น .pif เป็นต้น

ลำดับที่	ภัยพิบัติ	แนวทางปฏิบัติ/มาตรการควบคุม
๒ (ต่อ)	ภัยพิบัติที่เกิดจากความเสี่ยงด้าน Software เช่น ซอฟต์แวร์ระบบฐานข้อมูล/โปรแกรมหรือแอปพลิเคชันเสียหาย	(๕) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา (๖) ใช้ความระมัดระวังในการเปิด e-Mail ดังนี้ (๖.๑) อย่าเปิดไฟล์ e-Mail ถ้าไม่ทราบแหล่งที่มา (๖.๒) ลบ e-Mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา (๖.๓) Logout ออกจากระบบ e-Mail ทุกครั้งหลังจากเลิกใช้งาน (๗) ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จาก Internet ดังนี้ (๗.๑) ไม่ควรเปิดไฟล์ที่ไม่รู้จักที่แนบมากับโปรแกรมสนทนาต่าง ๆ เช่น Facebook, Twitter และ MSN เป็นต้น (๗.๒) ไม่ควรเข้าไปเปิด Website ที่แนะนำมาทาง e-Mail ที่ไม่ทราบแหล่งที่มา (๗.๓) ไม่ดาวน์โหลด ไฟล์ จาก Website ที่ไม่น่าเชื่อถือ (๗.๔) ติดตามข้อมูลการแจ้งเตือนการโจมตีของมัลแวร์ต่าง ๆ อย่างสม่ำเสมอ (๗.๕) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น ศทท. ต้องแจ้งข้อมูลเตือนภัยมัลแวร์คอมพิวเตอร์ผ่านระบบ Intranet ที่ http://intranet อย่างต่อเนื่องสม่ำเสมอ รวมทั้ง แนะนำวิธีการป้องกันและการกำจัดภัยที่เกิดจาก Software ดังกล่าว ให้เจ้าหน้าที่ได้ศึกษาและสามารถป้องกันและแก้ไขปัญหาในเบื้องต้นได้
๓	ภัยพิบัติที่เกิดจากความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ เช่น ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data room) ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า แผ่นดินไหว และน้ำท่วม) และเครื่องปรับอากาศห้องศูนย์ข้อมูลไม่ทำงาน	ศทท. ได้ดำเนินการ ดังนี้ **(๑)** ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า ศทท. ได้เลือกเพื่อฝึกปฏิบัติการในสถานการณ์จำลองในปีงบประมาณที่ผ่านมา พบว่าสามารถดำเนินการได้ตามเป้าหมายที่กำหนดไว้ และได้ดำเนินการ ดังนี้ (๑.๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) จำนวน ๒ เครื่อง เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวน ๒๖ เครื่อง ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งอุปกรณ์สำรองไฟฟ้าที่ใช้ควบคุมระบบเครือข่ายของ สนข. สามารถสำรองไฟฟ้าเพื่อใช้งานได้นานประมาณ ๔๐ นาที (๑.๒) เปิดอุปกรณ์สำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาอุปกรณ์สำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ (๑.๓) เมื่อเกิดกระแสไฟฟ้าดับ หากมีอุปกรณ์สำรองไฟฟ้าใช้งานอยู่ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ด้วย **(๒) การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data room)** (๒.๑) ศทท. ได้ดำเนินการติดตั้งระบบดับเพลิงแบบอัตโนมัติแล้วเสร็จ โดยใช้สารสะอาดที่สามารถดับเพลิงในห้องศูนย์ข้อมูลได้ภายในไม่เกิน ๒๐ นาที

ลำดับที่	ภัยพิบัติ	แนวทางปฏิบัติ/มาตรการควบคุม
๓ (ต่อ)	ภัยพิบัติที่เกิดจากความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ เช่น ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ถูกตัดกระแสไฟฟ้า การเกิดเพลิงไหม้ห้องศูนย์ข้อมูล (Data room) ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า แผ่นดินไหว และน้ำท่วม) และเครื่องปรับอากาศห้องศูนย์ข้อมูลไม่ทำงาน (ต่อ)	(๒.๒) ติดตั้งอุปกรณ์ดับเพลิง ทุกชั้นของอาคารและที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ควบคุมเพลิงในเบื้องต้น ในกรณีเหตุไฟไหม้ ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ **๓) ความเสียหายจากภัยพิบัติ/ภัยธรรมชาติ เช่น ฟ้าผ่า แผ่นดินไหว และน้ำท่วม)** (๓.๑) ตรวจสอบการติดตั้ง/จัดวางอุปกรณ์ต่าง ๆ ทั้งภายนอกและภายในตู้ Rack ทั้งหมด ทุก ๓ เดือน (๓.๒) ตรวจสอบความพร้อมใช้งานของระบบดับเพลิงและระบบเตือนภัย (Warning system) ทุก ๓ เดือน **(๔) เครื่องปรับอากาศห้องศูนย์ข้อมูลไม่ทำงาน** ตรวจสอบความพร้อมใช้งานของเครื่องปรับอากาศทุก ๖ เดือน
๔	**ภัยพิบัติที่เกิดจากความเสี่ยงด้านระบบเครือข่ายและ Internet** เช่น ระบบเครือข่ายหลักเสียหาย/ขัดข้อง ไม่สามารถใช้งานได้	ศทท. ได้มีการหมั่นตรวจสอบระบบเครือข่ายสื่อสารหลัก การจัดทำเส้นทางออกสู่เครือข่ายอินเทอร์เน็ต (Gateway) มากกว่า ๑ ทาง และการบริหารจัดการ Bandwidth เพื่อควบคุมการใช้งานเครือข่ายให้มีประสิทธิภาพเพื่อให้การใช้งานของ สนข. ได้รับ Bandwidth สูงกว่าการใช้งานด้านอื่น ๆ รวมทั้ง ได้ดำเนินการ ดังนี้ (๑) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ของ สนข. ได้โดยจะเปิดใช้งาน Firewall ตลอดเวลา อย่างต่อเนื่อง (๒) มีเจ้าหน้าที่ดูแลระบบเครือข่ายทำการตรวจสอบปริมาณข้อมูลบนเครือข่าย Internet ขององค์กรเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศที่มีความถี่ในการเรียกใช้ผิดปกติ เพื่อสรุปหาสาเหตุและแนวทางป้องกันต่อไป
๕	**ภัยพิบัติที่เกิดจากความเสี่ยงด้านความมั่นคงปลอดภัย** เช่น ถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี การเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต ระบบคอมพิวเตอร์ถูกเจาะ (Hack) การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์ รวมทั้งการก่อความไม่สงบ/จลาจล	สนข. มีมาตรการควบคุมการเข้าออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่ายหากจำเป็นให้มีเจ้าหน้าที่ของกลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่ายศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจรเป็นผู้รับผิดชอบนำพาบุคคลเข้าไป ผ่านประตู เข้า - ออก ซึ่งมีการติดตั้งเครื่องสแกนลายนิ้วมือรวมทั้ง ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพื่อบันทึกการเข้า - ออกและการปฏิบัติงานในห้องปฏิบัติการคอมพิวเตอร์แม่ข่ายด้วย (๑) ถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี ศทท. ได้ติดตั้งและใช้งานโปรแกรมป้องกันมัลแวร์ที่มีลิขสิทธิ์ถูกต้องของหน่วยงาน และดำเนินการ Update ข้อมูลป้องกันมัลแวร์ให้เป็นปัจจุบัน (๒) การเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต ศทท. ได้จัดทำระบบป้องกันการเข้าถึงห้องศูนย์ข้อมูล โดยอนุญาต

ลำดับที่	ภัยพิบัติ	แนวทางปฏิบัติ/มาตรการควบคุม
๕ (ต่อ)	**ภัยพิบัติที่เกิดจากความเสี่ยงด้านความมั่นคงปลอดภัย** เช่น ถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี การเข้าถึงศูนย์ข้อมูลโดยไม่ได้รับอนุญาต ระบบคอมพิวเตอร์ถูกเจาะ (Hack) การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์ รวมทั้งการก่อความไม่สงบ/จลาจล (ต่อ)	เฉพาะเจ้าหน้าที่ผู้เกี่ยวข้องกับการบริหารจัดการเครื่อง Server และเจ้าหน้าที่ที่มีสิทธิ์เข้าใช้งานภายในห้องศูนย์ข้อมูล รวมทั้งติดตั้งระบบกล้อง CCTV เพื่อบันทึกภาพการ เข้า - ออก ภายในห้องไว้ด้วย (๓) ระบบคอมพิวเตอร์ถูกเจาะ (Hack) ศทท. ได้ดำเนินการ ดังนี้ (๓.๑) จากภายนอก (๓.๑.๑) ได้ป้องกันไม่ให้ความสูญเสียเกิดขึ้นโดยการติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย เป็นการป้องกันบุคคลหรือมัลแวร์คอมพิวเตอร์มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ รวมทั้ง ได้ติดตั้งและใช้งานโปรแกรมป้องกันมัลแวร์ที่มีลิขสิทธิ์ถูกต้องของหน่วยงาน และดำเนินการ Update ข้อมูลป้องกันมัลแวร์ให้เป็นปัจจุบัน (๓.๑.๒) หมั่นตรวจสอบ Policy และ Log ของ Firewall และ IPS/IDS อย่างสม่ำเสมอ (๓.๒) จากภายใน (๓.๒.๑) มีมาตรการ และกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่าง ๆ ที่มีลิขสิทธิ์ไม่ถูกต้องลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายของ สนข. เพื่อป้องกันมิให้หน่วยงานมีความเสี่ยงที่จะถูกเจาะระบบและถูกจารกรรมข้อมูล เพราะแฮกเกอร์สามารถใช้มัลแวร์เพื่อควบคุมโครงสร้างพื้นฐานที่สำคัญและข้อมูลที่สำคัญได้ (๓.๒.๒) การควบคุมด้วยระบบ Desktop Management (๔) การสำรองข้อมูล (Backup) และการกู้คืนข้อมูล (Recovery) ไม่สมบูรณ์ ดำเนินการทดสอบการกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศจาก Backup file ทุก ๖ เดือน (๕) การก่อความไม่สงบ/จลาจล (๕.๑) ตรวจสอบความพร้อมใช้งานของอุปกรณ์รักษาความปลอดภัย CCTV, Access control ทุก ๖ เดือน (๕.๒) ดำเนินการทดสอบการกู้คืนระบบสารสนเทศและข้อมูลสารสนเทศจาก Backup file ทุก ๖ เดือน

ลำดับที่	ภัยพิบัติ	แนวทางปฏิบัติ/มาตรการควบคุม
๖	**ภัยพิบัติที่เกิดจากความเสี่ยงด้านตัวบุคคลและการใช้งาน** เช่น การใช้งานระบบซอฟต์แวร์เถื่อนหรือซอฟต์แวร์ละเมิดลิขสิทธิ์ และการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ผิดวัตถุประสงค์ (ต่อ)	ศทท. ได้ติดตั้งและใช้งานโปรแกรมที่มีลิขสิทธิ์ถูกต้องของหน่วยงาน รวมทั้ง มีมาตรการและกฎระเบียบในการควบคุมมิให้มีการติดตั้งโปรแกรมต่าง ๆ ที่มีลิขสิทธิ์ไม่ถูกต้องลงบนเครื่องลูกข่ายที่เชื่อมโยงกับเครือข่ายของ สนข. และรายงานผลการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์ของผู้ใช้งาน รวมทั้ง ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบ IT ดังนี้ ๑) ชี้แจงเจ้าหน้าที่ของหน่วยงานใน สนข. ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดภัยด้าน Human error ให้น้อยที่สุด เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น
		(๒) กำหนดแนวทางปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบ IT ดังนี้ (๒.๑) การตั้งค่าระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายให้มีการสำรองข้อมูลโดยอัตโนมัติเป็นประจำทุกสัปดาห์ (๒.๒) การสำรองข้อมูลไว้ใน CD, DVD และ/หรือสื่อบันทึกข้อมูลอื่น ๆ

บทที่ ๓
การจัดเตรียมอุปกรณ์และข้อควรปฏิบัติในการแก้ไข

๓.๑ การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมความพร้อมรับสถานการณ์ความไม่แน่นอนและภัยพิบัติที่จะเกิดขึ้นกับระบบ IT ของ สนข. นั้น ศทท. ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของ สนข. ได้จัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็น ในกรณีระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ขัดข้อง ใช้งานไม่ได้ โดยมีการจัดเตรียมอุปกรณ์ ดังนี้

๓.๑.๑ แผ่น Boot Disk สำหรับเปิดใช้งานเครื่องคอมพิวเตอร์ในกรณีที่ระบบปฏิบัติการเสียหาย

๓.๑.๒ แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

๓.๑.๓ แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

๓.๑.๔ แผ่นโปรแกรม Antivirus/Spyware

๓.๑.๕ แผ่น Driver อุปกรณ์ต่าง ๆ

๓.๑.๖ ระบบสำรองไฟฉุกเฉิน

๓.๑.๗ อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๓.๒ ข้อควรปฏิบัติในการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติหรือการใช้งานระบบเครือข่ายขัดข้อง

๓.๒.๑ กรณีเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๓.๒.๑.๑ กรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานระบบ IT ได้ตามปกติ ให้เจ้าหน้าที่แจ้งเหตุให้เจ้าหน้าที่กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย ศทท. ทราบทางโทรศัพท์ภายในหมายเลข ๔๕๑๔, ๔๐๘๑, ๔๕๑๕, ๔๐๑๓, ๔๐๑๒ และ ๔๕๑๓ เข้าไปดำเนินการแก้ไขหรือกรณีมีเหตุอันทำให้กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่ายไม่สามารถให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ได้ กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่ายจะต้องประกาศให้ทุกหน่วยของ สนข. ทราบทั่วกันโดยเร็วที่สุด

๓.๒.๑.๒ กรณีเกิดการขัดข้องเนื่องจากเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์ ให้เจ้าหน้าที่ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องคอมพิวเตอร์โดยเร็ว เพื่อป้องกัน ความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย

๓.๒.๑.๓ กรณีที่เกรงว่าเหตุขัดข้องที่เกิดขึ้นจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงาน ภายในอาคารสถานที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๓.๒.๑.๔ ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด และ/หรือ

๓.๒.๑.๕ ขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๓.๒.๑.๖ ให้เจ้าหน้าที่ผู้ดูแลระบบ กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย ศทท. ที่รับผิดชอบแจ้งเหตุขัดข้องนั้นให้หัวหน้ากลุ่มฯ ผอ.ศทท. และ CIO ทราบโดยเร็วที่สุด

๓.๒.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่าย

๓.๒.๒.๑ ปิดการเชื่อมต่อระบบเครือข่ายโดยเร็ว โดยปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๓.๒.๒.๒ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓.๒.๒.๓ ปิดระบบจ่ายไฟฟ้า ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดคุมเพลิงโดยเร็ว

๓.๒.๒.๔ รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๓.๒.๒.๕ ประสานขอความช่วยเหลือกับผู้ที่รับผิดชอบดูแลและบำรุงรักษาระบบเครื่องคอมพิวเตอร์แม่ข่ายและ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๓.๒.๒.๖ ในกรณีที่อุปกรณ์ด้าน Hardware เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้ผู้ที่รับผิดชอบบำรุงรักษาระบบ นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๓.๒.๒.๗ ผู้ดูแลระบบ กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย ต้องรีบแจ้งให้หัวหน้ากลุ่มฯ ผอ.ศทท. และ CIO ทราบโดยเร็วที่สุด

๓.๒.๓ กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการ ดังนี้

๓.๒.๓.๑ กรณีที่เครื่องคอมพิวเตอร์ฯ มีโปรแกรมป้องกันไวรัสอยู่แล้ว ให้ดำเนินการ Update ข้อมูล Antivirus ให้เป็นปัจจุบัน แล้ว Scan ไวรัส

๓.๒.๓.๒ กรณีที่เครื่องคอมพิวเตอร์ฯ ไม่มีโปรแกรมป้องกันไวรัส ให้ดำเนินการติดตั้งและใช้งานโปรแกรม Antivirus ที่มีลิขสิทธิ์ถูกต้องของหน่วยงาน และดำเนินการ Update ข้อมูล Antivirus ให้เป็นปัจจุบัน แล้ว Scan ไวรัส

๓.๒.๔ กรณีเมนบอร์ด (Main board) เสียหาย ให้ดำเนินการ ดังนี้

๓.๒.๔.๑ ให้จัดหาเมนบอร์ดมาเปลี่ยน

๓.๒.๔.๒ ติดตั้งเมนบอร์ดใหม่แทน

๓.๒.๔.๓ ทำการ Boot ระบบให้ใช้งานตามปกติ

๓.๒.๕ กรณีฮาร์ดดิสค์เสียหาย ให้ดำเนินการ ดังนี้

๓.๒.๕.๑ จัดหาฮาร์ดดิสค์ มาเปลี่ยน

๓.๒.๕.๒ ติดตั้งระบบปฏิบัติการ และระบบเครือข่าย รวมทั้งโปรแกรมประยุกต์ที่จำเป็นต่อการใช้งาน

๓.๒.๕.๓ นำข้อมูลที่ Backup ไว้มาทำการ Recovery เพื่อนำข้อมูลเดิมกลับมาใช้

๓.๒.๕.๔ ตรวจสอบและเปิดเครื่องคอมพิวเตอร์ให้ทำงานตามปกติ

บทที่ ๔

แผนปฏิบัติการเพื่อให้ระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณใช้งานได้อย่างต่อเนื่องภายหลังจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้าน IT และแผนการฝึกปฏิบัติการในสถานการณ์จำลองตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๔

๔.๑ การกำหนดหน้าที่ของบุคลากรผู้รับผิดชอบการดำเนินงานเพื่อแก้ไขปัญหาระบบ IT ของ สนข. ที่เกิดจากภัยพิบัติเพื่อให้ใช้งานได้อย่างรวดเร็ว ต่อเนื่อง และมีประสิทธิภาพ มีดังนี้

Chief Information Officer (CIO)
นางวิไลรัตน์ ศิริโสภณศิลป์ (๒๐๐๐)
รอง ผอ.สนข. : ทำหน้าที่ CIO

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
(ผอ.ศทท.) (๔๐๐๘)

ผู้กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวน วางแผน ติดตามและประเมินผลการจัดหาอุปกรณ์คอมพิวเตอร์และเครือข่าย
นายสมชาย ภูนาสี (๔๕๑๔)
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย

ผู้ประสานงานดูแลความพร้อมของระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์
นายสมชาย ภูนาสี (๔๕๑๔)
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย

ผู้ดูแลอุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และความปลอดภัยของฐานข้อมูลทั้งหมด รวมทั้งการทำสำเนาฐานข้อมูล
- นายนฤทธิ์ มัยรัตน์ นักวิชาการคอมพิวเตอร์ชำนาญการ (๔๕๑๕)
- นายพิสิฏฐ์ ป้อมทอง นักวิชาการคอมพิวเตอร์ปฏิบัติการ (๔๐๑๒)
- นางสาวนิปริน คำแสง นักวิชาการคอมพิวเตอร์ชำนาญการ (๔๐๘๑)
- นายชัยวัฒน์ ธรรมาสถิตนุกุล นักวิชาการคอมพิวเตอร์ปฏิบัติการ (๔๐๑๔)

ผู้รับผิดชอบดูแลและบำรุงรักษาระบบงานบริหารสำนักงานอัตโนมัติ (e-Office) และระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)
- นายพิสิฏฐ์ ป้อมทอง นักวิชาการคอมพิวเตอร์ปฏิบัติการ (๔๐๑๒)
- นางสาวนิปริน คำแสง นักวิชาการคอมพิวเตอร์ชำนาญการ (๔๐๘๑)
- นายชัยวัฒน์ ธรรมาสถิตนุกุล นักวิชาการคอมพิวเตอร์ปฏิบัติการ (๔๐๑๔)

ผู้รับผิดชอบการบริหารจัดการระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server)
- นายนฤทธิ์ มัยรัตน์ นักวิชาการคอมพิวเตอร์ชำนาญการ (๔๕๑๕)
- นายพิสุทธิ นิลม่วง พนักงานบริการเอกสารทั่วไป ระดับ ปวช (๔๕๑๓)
- นายชัยวัฒน์ ธรรมาสถิตนุกุล นักวิชาการคอมพิวเตอร์ปฏิบัติการ (๔๐๑๔)

ผู้รับผิดชอบดูแลและบำรุงรักษาคอมพิวเตอร์และอุปกรณ์ต่อพ่วง
- นายนฤทธิ์ มัยรัตน์ นักวิชาการคอมพิวเตอร์ชำนาญการ (๔๕๑๕)
- นายพิสิฏฐ์ ป้อมทอง นักวิชาการคอมพิวเตอร์ปฏิบัติการ (๔๐๑๒)
- นายทนงชัย ยศชัยพงศ์ นายช่างเขียนแบบชำนาญงาน (๔๕๑๓)
- นายพิสุทธิ นิลม่วง พนักงานบริการเอกสารทั่วไป ระดับ ปวช (๔๕๑๓)
- นายชัยวัฒน์ ธรรมาสถิตนุกุล นักวิชาการคอมพิวเตอร์ปฏิบัติการ (๔๐๑๔)

๔.๒ การจัดองค์กรปฏิบัติการฉุกเฉินในระบบสารสนเทศ สนข.

การจัดองค์กรปฏิบัติการฉุกเฉิน หรือสายการบังคับบัญชา (Lines of authority) เมื่อเกิดเหตุฉุกเฉิน

๔.๒.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

๔.๒.๑.๑ กำหนดนโยบายด้าน ICT และการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ

๔.๒.๑.๒ ให้คำปรึกษาแก่ ผอ.ศทท. ในการระงับเหตุฉุกเฉินระบบสารสนเทศ

๔.๒.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร

๔.๒.๒.๑ เป็นผู้อำนวยการในการระงับเหตุฉุกเฉินระบบสารสนเทศ

๔.๒.๒.๒ มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

๔.๒.๒.๓ มีอำนาจสั่งทำลายกุญแจ สถานที่เก็บวัตถุอันตรายเพื่อระงับเหตุฉุกเฉิน

๔.๒.๒.๔ ประชุมหารือกับผู้รับผิดชอบบริหารจัดการระบบเครือข่ายคอมพิวเตอร์

๔.๒.๒.๕ ประเมินสถานการณ์ และสั่งการให้ปรับแผนฯ ตามความเหมาะสม

๔.๒.๒.๖ รายงานข้อมูลและผลการปฏิบัติงานให้ CIO ทราบ

๔.๒.๓ ผู้กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวน วางแผน ติดตามและประเมินผลการจัดหาอุปกรณ์คอมพิวเตอร์และเครือข่าย หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย

๔.๒.๓.๑ วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อ ผอ.ศทท.

๔.๒.๓.๒ มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่า ผอ.ศทท. ซึ่งเป็นผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

๔.๒.๓.๓ สั่งการให้ผู้เกี่ยวข้องมาปฏิบัติตามแผนฯ

๔.๒.๓.๔ กำกับดูแลการปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวน วางแผน ติดตามและประเมินผลการจัดหาอุปกรณ์คอมพิวเตอร์และเครือข่าย

๔.๒.๓.๕ ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย

๔.๒.๔ ผู้ประสานงานดูแลความพร้อมของระบบระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์

๔.๒.๔.๑ ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง

๔.๒.๔.๒ รายงานให้ผู้อำนวยการระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

๔.๒.๔.๓ กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติม ในอนาคต

๔.๒.๔.๔ ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๔.๒.๕ ผู้ดูแลระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์และผู้ช่วยดูแลระบบ รวมทั้งผู้รับผิดชอบดูแลและบริหารจัดการระบบงานอื่น ๆ (Computer system and Computer network administrator and staffs) ต้องดำเนินการ ดังนี้

๔.๒.๕.๑ ตรวจสอบสาเหตุที่เกิดขึ้น

๔.๒.๕.๒ แจ้งผู้บังคับบัญชา

๔.๒.๕.๓ ดำเนินการแก้ไขหรือแจ้งผู้เกี่ยวข้องดำเนินการ

(๑) กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้ามาทำการดับเพลิง

(๒) พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่น ๆ มาช่วย

(๓) ปิดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

(๔) ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

๔.๒.๕.๔ หลังจากเกิดเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้หัวหน้ากลุ่มฯ ผอ.ศทท. และ CIO ทราบ โดยอุปกรณ์และรายการที่ต้องตรวจสอบ ได้แก่

(๑) ทำการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย

(๒) ทำการตรวจสอบ Virus, Worm, และ Spy ware

(๓) ทำการตรวจสอบ UPS

(๔) ทำการตรวจสอบ Transaction log files

(๕) ทำการตรวจสอบการใช้งานฐานข้อมูลระบบงานที่สำคัญ

(๖) ทำการตรวจสอบการเปลี่ยนแปลงของ Files ต่าง ๆ

(๗) ทำการตรวจสอบความถูกต้องของ Files ข้อมูล

(๘) ทำการตรวจสอบค่า Configuration ของระบบ

(๙) ตรวจสอบอุปกรณ์ที่จำเป็นต่าง ๆ ที่กำหนดไว้ให้พร้อมใช้งาน

๔.๒.๕.๕ เตรียมเครื่องมือ อุปกรณ์ ทั้งด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

๔.๒.๕.๖ ประสานงานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่ปรึกษาในการกู้ข้อมูล

๔.๒.๕.๗ ทำการสำรองข้อมูล ดังนี้

(๑) ทุกวันจันทร์ - วันพฤหัสบดี ทำการสำรองข้อมูลในส่วนของข้อมูล (Data)

(๒) ทุกวันศุกร์ทำการสำรองข้อมูลทั้งระบบ

๔.๒.๕.๘ ต้องเก็บสิ่งสำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ ได้แก่ โปรแกรมและแฟ้มข้อมูล Tape backup รายชื่อโปรแกรมเอกสารที่เกี่ยวข้องกับระบบปฏิบัติการและโปรแกรม รายการ Hardware สำรอง และสำเนาคู่มือ

๔.๒.๕.๙ นำระบบสำรองข้อมูลออกมาใช้งานเพื่อให้ระบบสามารถดำเนินการต่อไปได้

๔.๓ การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณภายหลังจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้าน IT

ระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณเป็นหัวใจหลักของการให้บริการระบบ IT ของ สนข. โดยปกติจะต้องอยู่ ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆ ได้ตลอด ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้ได้โดยเร็วที่สุดเท่าที่จะทำได้ เนื่องจากเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณต้องทำงานด้านบริการให้กับเครื่องลูกข่ายให้สามารถใช้งานได้ปกติ โดยต้องดำเนินการตรวจสอบสาเหตุที่เกิดขึ้น ดังนี้

๔.๓.๑ ในกรณีที่เป็น Hardware ต้องดำเนินการ ดังนี้

๔.๓.๑.๑ จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๔.๓.๑.๒ เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๔.๓.๑.๓ ในกรณีที่จัดหาไม่ทัน ให้ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๔.๓.๑.๔ ทีมกู้ระบบ (ผู้ดูแลระบบ นักวิชาการคอมพิวเตอร์ และทีมงานจากบริษัทที่ดูแล และบำรุงรักษาระบบฯ) ดำเนินการกู้ระบบกลับมาโดยเร็ว โดยนำ Backup tape / CD-ROM / Hard disk หรืออุปกรณ์สำรองข้อมูลอื่น ๆ ที่ได้สำรองข้อมูลไว้ นำกลับมาทำการ Recovery ข้อมูลให้ใช้งานระบบต่อไปได้

๔.๓.๑.๕ ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูลสารสนเทศ ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ รวมทั้งระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวข้อง อย่างสม่ำเสมอ

๔.๓.๑.๖ จัดทำรายงานผลการตรวจสอบและทดสอบระบบเสนอต่อ ผอ.ศทท. และ CIO

๔.๓.๒ ในกรณีที่เป็น Software ต้องดำเนินการ ดังนี้

๔.๓.๒.๑ ทีมกู้ระบบ (ผู้ดูแลระบบ นักวิชาการคอมพิวเตอร์ และทีมงานจากบริษัทที่ดูแล และบำรุงรักษาระบบฯ) ดำเนินการกู้ระบบกลับมาโดยเร็ว โดยนำ Backup tape / CD-ROM / Hard disk หรืออุปกรณ์สำรองข้อมูลอื่น ๆ ที่ได้สำรองข้อมูลไว้ นำกลับมาทำการ Recovery ข้อมูลให้ใช้งานระบบต่อไปได้

๔.๓.๒.๒ ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูลสารสนเทศ ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ รวมทั้งระบบเครือข่ายคอมพิวเตอร์ที่เกี่ยวข้อง อย่างสม่ำเสมอ

๔.๓.๒.๓ จัดทำรายงานผลการตรวจสอบและทดสอบระบบเสนอต่อ ผอ.ศทท. และ CIO

๔.๔ แผนการฝึกปฏิบัติการในสถานการณ์จำลองตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๓

๔.๔.๑ กรณีกระแสไฟฟ้าขัดข้อง

๔.๔.๒ กรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี

การจำลองสถานการณ์

การฝึกปฏิบัติการในสถานการณ์จำลองตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของ สนข.

กรณีกระแสไฟฟ้าขัดข้อง

โดยศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร

ในวันที่ ... ประมาณเดือน ก.ค. ๒๕๖๔

ผู้ดูแลและควบคุมการฝึกปฏิบัติการ : นายสมชาย ภูนาสี หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย (หน.กพค.)

ลำดับที่	เวลา กรณีกระแสไฟฟ้าขัดข้อง **ระหว่างเวลา ๑๑.๐๐ - ๑๒.๐๐ น.**	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
๑	๙.๓๐ - ๑๐.๓๐ น.	**กรณีกระแสไฟฟ้าขัดข้อง** ๑. เป็นการประชุมเตรียมการทีมฝึกปฏิบัติบนโต๊ะ (Table Top) ก่อนการฝึกปฏิบัติการในสถานการณ์จำลอง	ห้องประชุม ๔๐๒ อาคาร สนข.	ซักซ้อมความเข้าใจร่วมกัน - วิธีการปฏิบัติ - ระยะเวลา - ผู้รับผิดชอบ	กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย			
	๑๐.๔๕ น.	๒. ประกาศเพื่อให้เจ้าหน้าที่ สนข. ทราบการฝึกปฏิบัติฯ **(ตั้งแต่ ๑๑.๐๐ - ๑๒.๐๐ น.)**		- ติดต่อฝ่ายประชาสัมพันธ์ - จัดเตรียมประกาศ - ประกาศ	น.ส. นิปริน คำแสง			
	๑๑.๐๐ น.	๓. **ปิด** Breaker กระแสไฟฟ้าในห้อง Server		- ติดต่อกลุ่มบริหารพัสดุ เพื่อแจ้งขอดำเนินการ - ปิด Breaker ที่กำหนดไว้	นายพิสุทธิ นิลม่วง			
	๑๑.๐๑ น.	๔. ปิด Server / อุปกรณ์เครือข่าย เรียงตามลำดับ ๔.๑ เครื่อง Server ๔.๒ อุปกรณ์เครือข่าย ๔.๓ อุปกรณ์อื่น ๆ	อุปกรณ์, ระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายภายในห้อง Server	<u>ปิดเครื่อง Server</u> โดยมีขั้นตอน ดังนี้ โดยปิดตามลำดับ ดังนี้ ๑. AD Server เครื่องที่ ๑ และ AD Server เครื่องที่ ๒ โดยมีขั้นตอน ดังนี้ - ระบุ Username และ Password - Shutdown	นายนฤทธิ์ มัยรัตน์			

ลำดับที่	เวลา	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
				๒. e-Office Application Server เครื่องที่ ๑,	นายพิสิฏฐ์ ป้อมทอง			
				e-Office Application Server เครื่องที่ ๒,	นายพิสิฏฐ์ ป้อมทอง			
				e-Office Document Server,	นายพิสิฏฐ์ ป้อมทอง			
				e-Office Database Server	นายพิสิฏฐ์ ป้อมทอง			
				Logistics Application Server,	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				Logistics Database Server,	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				และ Logistics Cost Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				TDMC Server,	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				TDML ๑ Server,	น.ส. นิปริน คำแสง			
				TDML ๒ Server,	น.ส. นิปริน คำแสง			
				E-monitor Server,	น.ส. นิปริน คำแสง			
				Traffregion Server	น.ส. นิปริน คำแสง			
				และระบบ HR Server โดยมีขั้นตอนดังนี้	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				- กดปุ่ม Start				
				- Shutdown				
				๓. Altiris Server เครื่องที่ ๑, และ Altiris Server เครื่องที่ ๒,	นายนฤทธิ์ มัยรัตน์			
				kaspersky Server เครื่องที่ ๑, และ kaspersky Server เครื่องที่ ๒ โดยมีขั้นตอน ดังนี้	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				- ระบุ Username และ Password				
				- Shutdown				

ลำดับที่	เวลา	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
				<u>ปิดอุปกรณ์เครือข่าย</u> ตามลำดับ ดังนี้ ๑. Router : Cisco ๒๘๐๐ - เมื่อปิดสวิทช์ UPS อุปกรณ์ Router จะ Shutdown ทันที ๒. DNS/DHCP : Blue Cat ๒.๑ เลือกโปรแกรม Adonis Management Control ๒.๒ เลือก Menu Server ๒.๓ เลือก Server Control ๒.๔ เลือก Shutdown Server ๒.๕ ปิดสวิทช์ DNS/DHCP ๓. Wireless Control : Aruba - เมื่อปิดสวิทช์ UPS อุปกรณ์ Wireless Control จะ Shutdown ทันที ๔. Core Switch : Cisco Model Catalyst ๔๕๐๐ E - เมื่อปิดสวิทช์ UPS อุปกรณ์ Core Switch จะ Shutdown ทันที ๕. Firewall : Fortinet ๕.๑ ไปหน้า Web ด้วยหมายเลข IP http://๑๙๒.๑๖๘.๐.๒:๔๔๔๔ ๕.๒ เลือก Menu Shutdown ๕.๓ ปิดสวิทช์ Firewall	นายนฤทธิ์ มัยรัตน์ นายนฤทธิ์ มัยรัตน์ นายนฤทธิ์ มัยรัตน์ นายนฤทธิ์ มัยรัตน์			

ลำดับที่	เวลา	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
				<u>ปิดอุปกรณ์อื่น ๆ</u> UPS จำนวน ๒ เครื่อง โดยมีขั้นตอน ดังนี้ - กดปุ่มปิดสวิทช์ UPS โดยเปิดตามลำดับ ดังนี้ ๑. UPS เครื่องที่ ๑ ๒. UPS เครื่องที่ ๒ <u>ปิดสวิทช์</u> Router, IPS, Wireless Control และ Core Switch	นายทนงชัย ยศชัยพงศ์			
	๑๑.๒๒ น.	๕. ตรวจสอบความเรียบร้อย		- ตรวจสอบว่าอุปกรณ์ต่าง ๆ ปิดเรียบร้อยแล้ว	นายนฤทธิ์ มัยรัตน์ นายพิสิฏฐ์ ป้อมทอง น.ส. นิปริน คำแสง นายชัยวัฒน์ ธรรมาสถิตนุกุล นายทนงชัย ยศชัยพงศ์ นายพิสุทธิ นิลม่วง			
	๑๑.๒๘ - ๑๑.๓๑ น.	๖. รายงานผลต่อ ผอ.ศทท.	ศทท.	เมื่อดำเนินการ**ปิด**อุปกรณ์ต่าง ๆ แล้วเสร็จ	หน.กพค.			
	๑๑.๓๒ น.	๗. เมื่อกระแสไฟฟ้ากลับคืนสู่สภาวะปกติ **- เปิด** Breaker กระแสไฟฟ้าของห้อง Server		**เปิด** Breaker กระแสไฟฟ้าของห้อง Server	นายพิสุทธิ นิลม่วง			
	๑๑.๓๓ - ๑๑.๔๘ น.	๘. เปิดอุปกรณ์ของระบบคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายตามลำดับ ดังนี้ ๘.๑ อุปกรณ์อื่น ๆ ๘.๒ อุปกรณ์เครือข่าย ๘.๓ เครื่อง Server		<u>เปิดอุปกรณ์อื่น ๆ</u> UPS จำนวน ๒ เครื่อง โดยมีขั้นตอน ดังนี้ - เมื่อเปิดสวิทช์ UPS อุปกรณ์จะทำงานทันที โดยเปิดตามลำดับ ดังนี้ ๑. UPS เครื่องที่ ๑ ๒. UPS เครื่องที่ ๒	นายทนงชัย ยศชัยพงศ์			

ลำดับที่	เวลา	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
				<u>เปิดอุปกรณ์เครือข่าย</u> ตามลำดับ ดังนี้				
				๑. Router : Cisco ๒๘๐๐ โดยมีขั้นตอนดังนี้	นายนฤทธิ์ มัยรัตน์			
				- เมื่อเปิดสวิทช์ Router อุปกรณ์จะทำงานทันที				
				๒. DNS/DHCP : Blue Cat โดยมีขั้นตอนดังนี้	นายนฤทธิ์ มัยรัตน์			
				- เมื่อเปิดสวิทช์ DNS/DHCP อุปกรณ์จะทำงานทันที				
				๓. Wireless Control : Aruba โดยมีขั้นตอน ดังนี้	นายนฤทธิ์ มัยรัตน์			
				- เมื่อเปิดสวิทช์ Wireless Control อุปกรณ์จะทำงานทันที				
				๔. Core Switch : Cisco Model Catalyst ๔๕๐๐ E โดยมีขั้นตอน ดังนี้	นายนฤทธิ์ มัยรัตน์			
				- เมื่อเปิดสวิทช์ Core Switch อุปกรณ์จะทำงานทันที				
				๕. Firewall : Fortinet โดยมีขั้นตอน ดังนี้	นายนฤทธิ์ มัยรัตน์			
				- เมื่อเปิดสวิทช์ Firewall อุปกรณ์จะทำงานทันที				
				<u>เปิดเครื่อง Server</u> โดยมีขั้นตอน ดังนี้				
				- เมื่อเปิดสวิทช์ Server อุปกรณ์จะทำงานทันที				
				โดยเปิดตามลำดับ ดังนี้				
				๑. AD Server เครื่องที่ ๑	นายนฤทธิ์ มัยรัตน์			
				๒. AD Server เครื่องที่ ๒	นายนฤทธิ์ มัยรัตน์			

ลำดับที่	เวลา	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
				๓. e-Office Application Server เครื่องที่ ๑	นายพิสิฏฐ์ ป้อมทอง			
				๔. e-Office Application Server เครื่องที่ ๒	นายพิสิฏฐ์ ป้อมทอง			
				๕. e-Office Document Server	นายพิสิฏฐ์ ป้อมทอง			
				๖. e-Office Database Server	นายพิสิฏฐ์ ป้อมทอง			
				๗. Logistics Application Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๘. Logistics Database Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๙. Logistics Cost Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๑๐. TDMC Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๑๑. TDML ๑ Server	น.ส. นิปริน คำแสง			
				๑๒. TDML ๒ Server	น.ส. นิปริน คำแสง			
				๑๓. E-monitor Server	น.ส. นิปริน คำแสง			
				๑๔. Traffregion Server	น.ส. นิปริน คำแสง			
				๑๕. ระบบ HR Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๑๖. Altiris Server เครื่องที่ ๑	นายนฤทธิ์ มัยรัตน์			
				๑๗. Altiris Server เครื่องที่ ๒	นายนฤทธิ์ มัยรัตน์			
				๑๘. kaspersky Server เครื่องที่ ๑ ๑๙. kaspersky Server เครื่องที่	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๒๐. Intranet Server	นายนฤทธิ์ มัยรัตน์			
				๒๑. Web Server	นายนฤทธิ์ มัยรัตน์			
				๒๒. Sustainable transport Server	นายนฤทธิ์ มัยรัตน์			
				๒๓. Test Run Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๒๔. TDL๒ Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๒๕. TDCA File Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			
				๒๖. TDCA DB Server	นายชัยวัฒน์ ธรรมาสถิตนุกุล			

ลำดับที่	เวลา	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
	๑๑.๔๙ - ๑๑.๕๔ น.	๙. ตรวจสอบการทำงานของอุปกรณ์ / Server และอุปกรณ์ที่เกี่ยวข้อง		- Ping ไปสู่ IP ของอุปกรณ์ - ตรวจสอบการใช้งานเครื่อง e-Office Server และระบบสารสนเทศอื่น ๆ ได้แก่ TDML๑, TDML๒, ... เป็นต้น	น.ส. นิปริน คำแสง นายพิสิฏฐ์ ป้อมทอง นายนฤทธิ์ มัยรัตน์ นายชัยวัฒน์ ธรรมาสถิตนุกุล นายพิสุทธิ นิลม่วง			
	๑๑.๕๕ - ๑๑.๕๘ น.	๑๐. รายงานผลต่อ ผอ.ศทท.	ศทท.	เมื่อดำเนินการ**เปิด**อุปกรณ์ต่าง ๆ แล้วเสร็จ	หน.กพค.			
	๑๒.๐๐ น.	๑๑. ประกาศเพื่อให้เจ้าหน้าที่ สนข. ทราบถึงการสิ้นสุดการฝึกปฏิบัติฯ		- ติดต่อฝ่ายประชาสัมพันธ์ - จัดเตรียมประกาศ - ประกาศ	น.ส. นิปริน คำแสง			

การจำลองสถานการณ์
การฝึกปฏิบัติการในสถานการณ์จำลองตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของ สนข.
กรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี
โดยศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
ในวันที่ ... ประมาณเดือน ส.ค. ๒๕๖๔

ผู้ดูแลและควบคุมการฝึกปฏิบัติการ : นายสมชาย ภูนาสี หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย (หน.กพค.)

การฝึกปฏิบัติการฯ ครั้งนี้เป็นการฝึกปฏิบัติการฯ ทั่วทั้งองค์กรเพื่อให้บุคลากรของ สนข. มีส่วนร่วมในการฝึกปฏิบัติการฯ และเข้าใจขั้นตอนการฝึกปฏิบัติการดังกล่าว

๑. การดำเนินการก่อนการฝึกปฏิบัติการ

เจ้าหน้าที่ ศทท. (นางสาวนิปริน คำแสง) ประกาศเพื่อซักซ้อมความเข้าใจกับ User (สำนัก/กอง/ศูนย์/สำนักงานโครงการ/กตส./กพร.) ในการฝึกปฏิบัติตาม IT Contingency Plan ดังกล่าว

๒. การฝึกปฏิบัติการ มีดังนี้

ลำดับที่	เวลา กรณีกระแสไฟฟ้าขัดข้อง ระหว่างเวลา ๑๑.๐๐ - ๑๒.๐๐ น.	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
๑	๐๙๓๐-๑๐๓๐ น.	**กรณีถูกโปรแกรมมัลแวร์ประเภทต่าง ๆ โจมตี** ๑. เป็นการประชุมเตรียมการทีมฝึกปฏิบัติบนโต๊ะ (Table Top) ก่อนการฝึกปฏิบัติการในสถานการณ์จำลอง	ห้องประชุม ๔๐๒ อาคาร สนข.	ซักซ้อมความเข้าใจร่วมกัน - วิธีการปฏิบัติ - ระยะเวลา - ผู้รับผิดชอบ	กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย			
	๑๐.๔๕ น.	๒. ประกาศเพื่อให้เจ้าหน้าที่ สนข. ทราบการฝึกปฏิบัติฯ **(ตั้งแต่ ๑๑.๐๐ - ๑๒.๐๐ น.)**		- ติดต่อฝ่ายประชาสัมพันธ์ - จัดเตรียมประกาศ - ประกาศ	น.ส. นิปริน คำแสง			
	๑๑๐๐-๑๑๕๘ น.	๓. จำลองสถานการณ์ขณะนี้มีไวรัส ๓.๑ เจ้าหน้าที่ ศทท. ท่านหนึ่งได้โทรฯ หาเจ้าหน้าที่ ศทท. (กพค.)		- จัดเตรียมประกาศ - ประกาศ	ศทท. (กพค.) และ User			

ลำดับที่	เวลา กรณีกระแสไฟฟ้าขัดข้อง ระหว่างเวลา ๑๑.๐๐ - ๑๒.๐๐ น.	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
		เพื่อให้เจ้าหน้าที่ ศทท. (กพค.) ตรวจสอบเครื่องคอมพิวเตอร์ดังกล่าว ๓.๒ เจ้าหน้าที่ ศทท. (กพค.) ได้ตรวจสอบเครื่องคอมพิวเตอร์ดังกล่าวแล้ว พบว่าไวรัสดังกล่าวเป็นไวรัสชนิด Ransomware ซึ่งแพร่กระจายผ่านทางระบบเครือข่ายคอมพิวเตอร์และเป็นไวรัสชนิดที่โปรแกรม Antivirus ในปัจจุบันไม่สามารถตรวจพบได้ จึงต้องทำการดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์ดังกล่าวโดยเร็ว ๓.๓ ประกาศแจ้งบุคลากรของ สนข. ทุกท่านว่า “ขณะนี้เป็นการจำลองสถานการณ์การติดไวรัสของครื่องคอมพิวเตอร์ของเจ้าหน้าที่ ศทท. ท่านหนึ่ง จึงขอให้เจ้าหน้าที่ สนข. ทุกท่านโปรดตรวจสอบ		- จัดเตรียมประกาศ - ประกาศ				

ลำดับที่	เวลา กรณีกระแสไฟฟ้าขัดข้อง ระหว่างเวลา ๑๑.๐๐ - ๑๒.๐๐ น.	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
		ระบบคอมพิวเตอร์ของตนเองว่ามีสิ่งผิดปกติหรือไม่ เช่น แสดงข้อความ Digital file ที่ผิดปกติหรือไม่รู้จักแหล่งที่มา หรือเครื่องคอมพิวเตอร์ของท่านทำงานผิดปกติไปจากเดิม” ซึ่งไม่พบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติไปจากเดิม ๓.๔ เจ้าหน้าที่ ศทท. (กพค.) ดำเนินการ Format เครื่องที่ติดไวรัส แล้วดำเนินการดังนี้ (๑) ติดตั้งระบบปฏิบัติการและระบบเครือข่าย รวมทั้งโปรแกรมประยุกต์ที่จำเป็นต่อการใช้งาน พร้อมทั้งเสียบสาย LAN (๒) นำข้อมูลที่ Backup ไว้มาทำการ Recovery เพื่อนำข้อมูลเดิมกลับมาใช้ (๓) ตรวจสอบและเปิดเครื่องคอมพิวเตอร์ให้ทำงานตามปกติ						

ลำดับที่	เวลา กรณีกระแสไฟฟ้าขัดข้อง ระหว่างเวลา ๑๑.๐๐ - ๑๒.๐๐ น.	สถานการณ์จำลอง	สถานที่	วิธีการ/ขั้นตอนการปฏิบัติการ	ผู้รับผิดชอบ	ผลการปฏิบัติการ		หมายเหตุ
						สำเร็จ	ไม่สำเร็จ	
	๑๒.๐๐ น.	๔. ประกาศแจ้งสิ้นสุดการจำลองสถานการณ์เพื่อให้บุคลากรของ สนข. ทำงานได้ตามปกติ		- จัดเตรียมประกาศ - ประกาศ	น.ส. นิปริน คำแสง			

บทที่ ๕
ข้อเสนอแนะ

การจัดทำ IT Contingency Plan นั้น จัดทำขึ้นเพื่อเป็นแนวทางในการป้องกันและลดปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบ IT ของหน่วยงาน และเพื่อให้หน่วยงานสามารถใช้งานระบบ IT ได้อย่างต่อเนื่อง ซึ่งจากผลการวิเคราะห์ข้อมูลสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบ IT ของ สนข. พบว่ามาจาก ๖ ประเภทความเสี่ยง ได้แก่ ความเสี่ยงด้าน Hardware ความเสี่ยงด้าน Software ความเสี่ยงด้านภัยพิบัติ/ภัยธรรมชาติ ความเสี่ยงด้านระบบเครือข่ายและ Internet ความเสี่ยงด้านความมั่นคงปลอดภัย และความเสี่ยงด้านตัวบุคคลและการใช้งาน ซึ่งได้จัดทำแนวทางปฏิบัติและข้อควรปฏิบัติเพื่อเตรียมรับสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านต่าง ๆ ไว้แล้ว แต่เนื่องจากระบบ IT มีการพัฒนาและเปลี่ยนแปลงไปอยู่เสมอ ศทท. จึงเห็นสมควรให้มีการทบทวน IT Contingency Plan จำนวน ๑ ครั้ง/ปี และฝึกปฏิบัติการในสถานการณ์จำลองตาม IT Contingency Plan อย่างต่อเนื่อง อย่างน้อย ๑ ครั้ง/ปี และนำข้อมูลข้อเท็จจริงที่ได้จากการฝึกปฏิบัติการในสถานการณ์จำลองตาม IT Contingency Plan ของ สนข. ไปปรับปรุงการฝึกปฏิบัติการในสถานการณ์จำลองตาม IT Contingency Plan ของ สนข. ในปีถัดไป โดยนำข้อมูลผลการฝึกปฏิบัติการไปจัดทำเป็นสถิติเปรียบเทียบในแต่ละปีที่ทำการฝึก เพื่อให้ทราบถึงข้อมูลข้อเท็จจริงในการพัฒนากระบวนการและพัฒนาบุคลากรที่เกี่ยวข้องในการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศต่อไป